CLAIMS:

Having thus described the invention, what is claimed and desired to be secured by Letters Patent is:

1. A method of preventing unauthorized personnel access to a computer file used to perform a function on the computer comprising:

selecting a file;

inserting a key into the contents of the file; and,

encrypting the file after the key has been inserted using an encryption key.

2. The method of claim 1 in which the key is randomly inserted into the contents of the file.

3. The method of claim 2 in which the encryption key is a second key, separate from the first said key.

4. The method of claim 3 further including:

decrypting the encrypted file using the second key; and,

scanning the decrypted file to locate the first said key, the decrypted file then being validated for use to perform the function for which it is used if the first said key is found, but the decrypted file not being validated for use if the first said key is not found which is an indication that the file has been altered without authorization.

5. The method of claim 5 further including storing a copy of the file after it is encrypted using the second key and replacing the original file with the stored copy thereof if the first said key cannot be found after the file is decrypted, the replaced copy of the file then being used to perform the desired function.

6. The method of claim 1 in which the file is an operating system (OS) component file.

7. A method of preventing an unauthorized person access to an operating system (OS) file of a computer, comprising:

selecting an operating file;

inserting a first key into the contents of the file and then encrypting the resulting file using a second key;

subsequently decrypting the file using the second key and examining the decrypted file for the first key;

validating the decrypted file for use by the computer if the first key is found in the decrypted file; but,

rejecting the decrypted file for use by the computer if the first key is not found, because failure to find the first key is an indication the computer has been hacked.

8. The method of claim 7 in which the first key is randomly inserted into the contents of the file.

9. The method of claim 7 in which the second key is a key separate from the first key.

10. The method of claim 9 further including storing a copy of the file after it is encrypted using the second key and replacing the original file with the stored copy thereof if the first said key cannot be found after the file is decrypted, the replaced copy of the file then being used to perform the desired function.

11. The method of claim 7 which is implemented as a computer program.

12. The method of claim 11 in which the computer program is an add-in component to web server software.

13. The method of claim 11 in which the computer program is incorporated into a stand alone server that communicates with a web server.

14. The method of claim 11 in which the computer program is incorporated directly into a web server.

15. A method of preventing a hacked computer file from being run on a computer thereby to prevent damage caused by hacking, comprising:

selecting an program file run by the computer;

randomly inserting a first key into the contents of the file;

encrypting the resulting file using a second, separate key;

decrypting the encrypted file prior to its subsequent use, the file being decrypted using the second key and the decrypted file now being examined for the first key embedded therein; and,

validating the decrypted file for use by the computer if the first key is found in the decrypted file, but rejecting the decrypted file for use by the computer if the first key is not found because failure to find the first key in the decrypted file is evidence the file has been hacked.

16. The method of claim 15 further including storing a copy of the file after it is encrypted using the second key and replacing the original file with the stored copy thereof if the first said key cannot be found after the file is decrypted, the replaced copy of the file then being used to perform the desired function.

17. The method of claim 15 which is implemented as a computer program.

18. The method of claim 17 in which the computer program is an add-in component to web server software.

19. The method of claim 17 in which the computer program is incorporated into a stand alone server that communicates with a web server.

20. The method of claim 17 in which the computer program is incorporated directly into a web server.